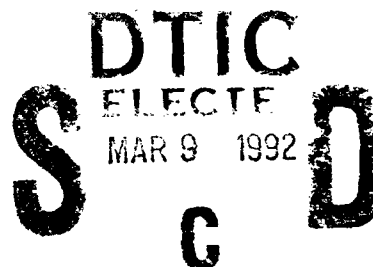




NATIONAL COMPUTER SECURITY CENTER

AD-A247 239



# FINAL EVALUATION REPORT

OF

## FISCHER INTERNATIONAL SYSTEMS CORPORATION

Watchdog /  
Watchdog Armor

92-05768



1 October 1990

Approved for Public Release:  
Distribution Unlimited

92 3 04 012

FINAL EVALUATION REPORT  
Fischer International Systems Corporation

Watchdog  
Version 5.2.2  
and  
Watchdog Armor



NATIONAL  
COMPUTER SECURITY CENTER

9800 Savage Road  
Fort George G. Meade  
Maryland 20755-6000

1 October 1990

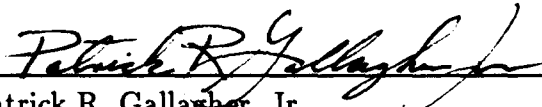
Report No. CSC-EPL-90/007  
Library No. S236,002

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

## FOREWORD

This publication, the Final Evaluation Report Fischer Watchdog is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the Fischer evaluation. The requirements stated in this report are taken from the *Computer Security Subsystem Interpretation* of the *Department of Defense Trusted Computer System Evaluation Criteria* dated 16 September 1988.

Approved:



---

Patrick R. Gallagher, Jr.  
National Security Agency /  
National Computer Security Center

1 October 1990

## ACKNOWLEDGEMENTS

### Team Members

Team members included the following individuals, who were provided by the following organization:

Howard Holm  
Walter K. Roddy

National Security Agency  
Trusted Product and Network Security Evaluation Division  
Fort George G. Meade, Maryland 20755-6000

# Contents

<b>FOREWORD</b>	<b>i</b>
<b>ACKNOWLEDGEMENTS</b>	<b>ii</b>
<b>EXECUTIVE SUMMARY</b>	<b>v</b>
<b>Chapter 1 Introduction</b>	<b>1</b>
Evaluation Process Background . . . . .	1
Subsystem Evaluation Program . . . . .	2
Document Organization . . . . .	2
<b>Chapter 2 System Overview</b>	<b>4</b>
Product History . . . . .	4
Product Overview . . . . .	4
Security Relevant Portion (SRP) . . . . .	4
Hardware Architecture . . . . .	5
Software Architecture . . . . .	5
SRP Protected Resources . . . . .	6
Subjects . . . . .	6
Objects . . . . .	7
SRP Protection Mechanisms . . . . .	7
Privileges . . . . .	7
Identification and Authentication . . . . .	8
Audit . . . . .	8
Discretionary Access Control . . . . .	9
Object Reuse . . . . .	10
<b>Chapter 3 Evaluation as a Subsystem</b>	<b>12</b>
Features . . . . .	12
Identification and Authentication . . . . .	12
Audit . . . . .	14
Discretionary Access Control . . . . .	17
Object Reuse . . . . .	19
Assurances . . . . .	20
System Architecture . . . . .	20
System Integrity . . . . .	23
Security Testing . . . . .	23
Documentation . . . . .	25
Security Features User's Guide . . . . .	25

Trusted Facility Manual . . . . .	26
Test Documentation . . . . .	27
Design Documentation . . . . .	27
Rating Assignment . . . . .	28
<b>Chapter 4 Evaluator's Comments</b>	<b>30</b>
<b>Appendix A Evaluated Hardware Components</b>	<b>31</b>
<b>Appendix B Evaluated Software Components</b>	<b>32</b>
<b>Appendix C Glossary of Acronyms</b>	<b>34</b>

## EXECUTIVE SUMMARY

The National Security Agency (NSA) / National Computer Security Center (NCSC) examined the security protection mechanisms provided by Fischer International Systems Corporation's Watchdog. Watchdog is a subsystem intended to provide additional security for personal computers, not a complete trusted computer system. It was therefore evaluated against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC). The computer security features evaluated were identification and authentication (I&A), discretionary access control (DAC), object reuse (OR), and audit (AUD).

The evaluation team determined that the highest rating at which Watchdog satisfies the DAC, I&A, and the audit requirements of the CSSI is class D2. Watchdog also performs some object reuse functions, but failed to meet all the feature requirements specified by the CSSI. Therefore, the object reuse feature received a rating of D.

To obtain the level of trust described in this report, Watchdog must be configured in accordance with the Trusted Facility Manual, or its equivalent, and properly administered. This includes restricting access to programming languages, compilers, debuggers, and other utilities for certain users. Watchdog accomplishes this by protecting system objects and restricting access to system resources.

Subsystems are intended to add a level of assurance to an automatic data processing (ADP) system that has limited or ineffective security mechanisms. Subsystems are not intended to protect any information on an ADP system which processes classified information because subsystems may not be capable of maintaining the integrity of classified information. Subsystems should not be added to a automatic data processing system for the sole purpose of processing classified or sensitive information.

# Introduction

In November 1989, the evaluation team began a product evaluation of Fischer International Systems Corporation's Watchdog. The objective of this evaluation was to rate Watchdog against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a final rating for each of Watchdog's features. This report documents the results of the evaluation. This evaluation applies to Watchdog version 5.2.2 available from Fischer International Systems Corporation.

Material for this report was gathered by the evaluation team through documentation, interaction with system developers, and use of Watchdog.

## Evaluation Process Background

The National Computer Security Center (NCSC), located within the National Security Agency (NSA) created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of Trust Technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program, the Center works with the manufacturers of hardware and software products to implement and make available to the public technically sound computer security solutions. Under this program, the NCSC evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.



## Subsystem Evaluation Program

The NCSC has recognized a need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class of the TCSEC. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations.

Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may be used as justification for processing classified material.

Subsystems considered in the subsystem evaluation program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria*. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog*.

## Document Organization

This report consists of four major chapters and three appendices. Chapter 1 is an introduction. Chapter 2 provides an overview of the system's hardware and software architecture.

Chapter 3 provides a mapping between the requirements specified in the CSSI and the features and assurances that fulfill those requirements. Chapter 4 presents the evaluation team's comments on the subsystem. The appendices identify specific hardware and software components to which the evaluation applies and a glossary of terms.

# System Overview

## Product History

Fischer International Systems Corporation is a privately held company which designs, develops, and markets software and related products for IBM mainframes and personal computers. Version 4.1 of Watchdog was previously evaluated and placed on the EPL.<sup>1</sup> Since the previously evaluated product, Fischer has made several significant security changes to the product. Some of these changes are the addition of resource restrictions, increased audit capability, and dual password logons.

## Product Overview

Watchdog was evaluated as a combination of Watchdog PC Data Security software version 5.2.2 and the Watchdog Armor card version 1.1.0. Throughout this report the label Watchdog will be used to refer to the combination of these two products, unless specifically stated otherwise. Watchdog provides domain isolation by providing DAC controlled menus which restrict users' access to objects. Watchdog provides identification and password controlled system access, thorough audit trails, and prevention of data scavenging of files. The Watchdog Armor card provides hardware boot protection, DES encryption, and a protected clock for reliable audit record-keeping.

## Security Relevant Portion (SRP)

The protection critical mechanism or the Security Relevant Portion (SRP) of Watchdog, consists of its hardware and software capabilities. A description of these mechanisms and their security relevant roles are described in the following two subsections.

---

<sup>1</sup> Final Evaluation Report of Fischer International Watchdog Version 4.1 dated 24 October 1986

## Hardware Architecture

The hardware architecture of Watchdog is based on the IBM PC/XT or IBM PC AT architecture. The hardware base must include a diskette drive and a fixed disk drive. Watchdog includes a small, half-height, circuit card, which is purchased separately from the Watchdog PC Data Security software. The card is marketed as Watchdog Armor. Functions included on the circuit card include diagnostics, boot protection, system clock, and hardware support for encryption.

Diagnostics for the base system are provided with the IBM hardware. The hardware diagnostics for Watchdog Armor are included with the circuit card. These diagnostics may be activated by the system administrator from the Watchdog Armor Administrator Program. The diagnostics verify the correct operation of the clock, RAM, and DES encryption hardware.

The hardware boot protection of Watchdog Armor prevents the booting of the PC from a removable media drive and redirects such attempts to boot to the fixed disk drive.

Watchdog Armor provides a system clock that is not generally subject to modification. This clock provides a more trusted reference for the audit functions of the system.

Hardware support for encryption<sup>2</sup> is provided by a DES chip on the Watchdog Armor Card. This greatly enhances the speed of the file system when DES encryption is being used.

## Software Architecture

This section describes the software relevant components of Watchdog's SRP.

Watchdog version 5.2.2 is designed to operate on PC's running MS-DOS or PC DOS versions 2.0 or higher.

Most of Watchdog's security functions are performed by its software. At system initialization, Watchdog locks out the keyboard and floppy drives so that the PC can be brought up under Watchdog's control. The first thing a user of the system will see is the Watchdog logon screen. It is through this mechanism that all users are identified and authenticated. Once authenticated, the user's ID is used throughout the system to determine access privileges.

After logging on to the system, Watchdog displays the user's area menu. This menu is established by the system administrator (SA), and displays only those directories which the user may access. Watchdog refers to these protected directories as areas. Each of these areas

---

<sup>2</sup>The NCSC team did not evaluate the strength of the encryption algorithms.

may have different access permissions for the user. Also, these areas may be shared with other users if the SA configures it this way.

Once the user logs onto the system, Watchdog audits his/her actions. Some audited events include logon/logoff, access to areas, and execution of programs. Watchdog also collects information about attempted security violations such as guessing passwords, attempting illegal access to areas and programs, excessive system usage, and attempting to tamper with the audit trail. Each user may view his/her own audit trail information, but may not view this information related to other users.

Watchdog software also determines whether a user has access privileges for system resources such as parallel ports, serial ports, and diskette drives.

The Watchdog software performs object reuse in the following two ways. When a user deletes a file, or reduces its size Watchdog zeroes out this freed space. Also, when a user logs off, Watchdog zeroes out all memory (real and EMS).

Watchdog provides some protection against accidental or malicious formatting of the hard disk. Watchdog also provides additional data protection by encrypting stored information. Watchdog supports DES and their own encryption algorithm.<sup>3</sup>

## SRP Protected Resources

This section describes the subjects and objects that Watchdog mediates access between.

### Subjects

The subjects are defined as:

- Users

Only the user who has been designated as the system administrator can access the SA program menu. The SA program is used to set up the security options of the Watchdog system. Through this protected program the SA grants access privileges for all other users of the system.

---

<sup>3</sup>The NCSC team did not evaluate the strength of the encryption algorithms.

## Objects

Watchdog's protected objects are the following:

The named objects:

- Files
- Directories and subdirectories
- Floppy Disk Drives
- Serial Ports
- Parallel Ports

The protected storage objects:

- Files
- Memory
- Message buffers
- Memory registers

## SRP Protection Mechanisms

This section describes Watchdog's privileges, I&A, DAC, OR, and Audit mechanisms.

### Privileges

Watchdog provides two levels of user privileges, the System Administrator (SA), and the Users. The SA performs his/her functions through interfacing with the trusted SA program. The System Administrator controls the privileges of all system users. The SA may grant similar access for more than one user to the same file(s). Users are not able to grant themselves, nor others, access to any objects on the system.

## Identification and Authentication

When the PC is booted Watchdog displays a logon screen on the terminal. The user is prompted for a user ID, one or two passwords, and possibly a project ID. The passwords may be up to twelve characters long and are case sensitive. If the system administrator has enabled multiple passwords, Watchdog will display a logon token after the first password. By verifying that the token is correct, a user may gain some assurance that the logon process is not being emulated by a user program before entering the second password. When the logon process is completed, the system will complete the boot process and leave the user at the DOS prompt or an area menu depending on the access allowed by the system administrator.

The system administrator may optionally require users to change their passwords at an interval of time from 1 to 999 days. The system administrator may also specify a minimum number of characters for user passwords up to the maximum of twelve. The system also allows configuration of an inactivity logout timer to automatically terminate the sessions of users who have left the system unattended.

The authentication data is stored in a directory accessible only to system administrators. This directory is protected by the DAC protection mechanisms of Watchdog (see page 9, "Discretionary Access Control.")

## Audit

Watchdog has the capability to record a variety of user actions in audit logs for review later by the system users. Although any user may generate an audit report, only the system administrator may generate reports that contain records of security violations and records generated by other user names. Instructions are given in the Trusted Facility Manual to remove the ability of unprivileged users to access the audit reporting features. Full audit reporting capabilities are only available through the SA program menu.

Audit data is stored in a directory accessible only to system administrators. This directory is protected by the DAC protection mechanisms of Watchdog (see page 9, "Discretionary Access Control.") A number of internal consistency checks are run to insure that the data has not been corrupted.

Auditable events include:

- System access - logon, logoff, or failed.
- File access - create, access, rename, or delete.

- Program access - running a program.
- Users guessing passwords.
- Continuous usage of more than 48 hours.
- Evidence of tampering with audit logs.
- Use of system administration utilities.

Auditable items are selected for auditing in varying ways depending on the actual item to be enabled or disabled. Auditing of file accesses is selective by file or directory. This is selectable in the utility used to set file access permissions. Auditing of most other events is selectable through the Change System Permissions menu, accessible through the System Profile menu of the SA program.

Audit reduction is performed by a menu driven program which produces a large number of tailored reports. Records to be reported may be selected by date, user ID, project ID, and program. The reports may be sorted by user ID, project ID, or date. Report formats may be saved for repeated use over time.

Each audit record contains the user ID, project ID, date information, the areas the user was logged in to access and information related to the specific event. Event specific information in the record includes the file or program accessed.

## Discretionary Access Control

Watchdog's DAC capability allows the system administrator to define a set of permissions for users of the PC. These permissions are divided into four general types: system, file access, resource, and utility. Each of these types will be discussed below.

System permissions are effective any time any user is on the system, regardless of the user's identity. These permissions are kept in the System Profile, which only the system administrator may change. Examples of system permissions are whether users will be required to periodically change their passwords, whether direct disk reads and writes will be prohibited, and whether to record login/logout date/time of users.

Resource permissions are set up in the User Profile, and may be different for each user. These permissions control access to DOS and input/output devices attached to the PC. The actual permissions are as follows:

- Access to DOS commands



- Access to diskette drive reads and writes
- Access to parallel ports
- Access to serial ports

Area access permissions are defined in the User Profile and the Area Profile (area is Watchdog's name for protected directories). The Area Profile defines access rights for all users of its directory, while the User Profile defines access rights for individual users. Access rights may be defined globally in the Area Profile by using the Global Allow or Global Deny options. These options apply to all users who access the area (directory) and override the User Profile permissions.

The SA may enter file access definitions through the System Profile menu. This option allows the SA to list the files each user may access along with the permissions granted for each file. This list is used by the audit trail mechanism to determine which specific files to track. The following file access rights are provided:

- READ - view a file, also implies execute
- WRITE - write to a file, user may not view file
- EXECUTE - execute a file/program, user may not copy or view file
- CREATE/DELETE - create new files, delete old files, user may not change existing files

Utilities are those DOS functions or utility programs which the system administrator may allow users to access. These utilities are displayed in the form of a utility menu, which varies for each user.

Users of the Watchdog system are only able to access those areas which the SA gives them privileges. Users are kept from accessing other user's areas through the use of a menuing structure. One can only perform those functions listed in one's menu.

## Object Reuse

Watchdog prevents the reuse of most storage objects on the system. Objects on the system are cleared on deallocation. This counters the ability of a user to examine data remaining from a previous session.

The ability to clear files is configurable by the system administrator utilizing the system profile menu of the SA program. If the "Enable Zeroing Deleted Files" option is selected, every file that is deleted will be overwritten with zeros.

Memory objects are cleared by Watchdog by overwriting main memory when a user's session is terminated. Terminate and Stay Resident (TSR) programs are decoupled from the keyboard during logon so that they may not be used until the system has authenticated the user. TSRs loaded by the system configuration files before user logon are not cleared by the system at each session termination.

## Evaluation as a Subsystem

This chapter presents the CSSI requirements and then explains how Watchdog satisfies them. The computer security features that were evaluated for the Watchdog product are Identification and Authentication (I&A), Discretionary Access Control (DAC), Audit (Aud), and Object Reuse (OR). For each feature, this chapter states the requirements, describes Watchdog's efforts to meet those requirements, and concludes with a statement as to the level of requirements that have been satisfied. This pattern is continued for each of the CSSI requirements for assurance and documentation. Finally, a rating assignment section (see page 28 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

### Features

#### Identification and Authentication

##### Requirement

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

##### Interpretation

###### - D1:

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A

subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

## **- D2:**

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

## **Applicable Features**

Watchdog requires that all users log in through the logon screen before taking any other actions. There are no apparent ways to circumvent this requirement. The user ID's are large enough to uniquely identify users and the system administrator. Authentication data is stored in the Watchdog system administrator's protected area and is not accessible to unauthorized users. The user's identification is passed along to the audit mechanism of Watchdog.

## **Conclusion**

Watchdog satisfies the Identification and Authentication D2 feature requirement.

## **Audit**

### **Requirement**

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity. The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.

### **Interpretation**

#### **- D2**

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied by auditing subsystems at AUD/D2.

##### **2.4.3.1.1 Creation and management of audit trail**

The auditing subsystem shall create and manage the audit trail of security-relevant events in the system. If the other portions of the system are unable to capture data about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store data about

events if the other portions of the system are capable of creating such data and passing them on.

#### **2.4.3.1.2 Protection of audit data**

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

#### **2.4.3.1.3 Access control to audit**

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

#### **2.4.3.1.4 Specific types of events**

Data about all security relevant events must be recorded. The other portion of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

#### **2.4.3.1.5 Specific information per event**

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

#### **2.4.3.1.6 Ability to selectively audit individuals**

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

**-D3:**

The following interpretation, in addition to the interpretation and requirement for AUD/D2, shall be satisfied for the AUD/D3 class.

**2.4.3.2.1 Real-time alarms**

The auditing subsystem shall provide the capability for the security administrator to set thresholds for certain auditable events. Furthermore, when the thresholds are exceeded, the audit subsystem shall immediately notify the security administrator of imminent security violation.

**Applicable Features**

Watchdog provides for the auditing of security relevant events within the system, and generation of reports by the system administrator. The audit reporting facility maintains records detailing the use of the I&A mechanism, the accessing of objects, and attempts to subvert the security of the system. For a detailed list of the auditable events see page 8, "Audit."

The system administrator may request reports by user and may tailor the information provided by the reports in a number of ways. The report may include the user, time, and other relevant information that was contained in the original audit record.

The audit data is maintained in system area and is inaccessible to unprivileged users except by use of the system audit facility which restricts access to a subset of the audit data. No unprivileged user may see another user's audit data. No unprivileged user may see any security critical events.

**Conclusion**

Watchdog satisfies the Audit D2 feature requirement. Watchdog does not fully satisfy the D3 feature requirement because it does not completely support the concept of real time analysis and response to security alarms. Although real-time, audible alarms are implemented, Watchdog cannot guarantee that it can "immediately notify the security administrator". Watchdog is not a networked product, and the security administrator is not simultaneously logged on as a user. The security administrator may not be physically close enough to monitor the beeps emanating from several different PC's, and it would be difficult for the security administrator to take any meaningful action.

## **Discretionary Access Control**

### **Requirement**

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of specifying, for each named object, a list of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

### **Interpretation**

#### **- D1:**

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

#### **2.1.3.1.1 Identified users and objects**

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/D1, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to: access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

#### **2.1.3.1.2 User-specified object sharing**

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).



### **2.1.3.1.3 Mediation**

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows access.

#### **- D2:**

The following interpretations, in addition to the interpretations for the DAC/D1 Class, shall be satisfied at the DAC/D2 Class.

### **2.1.3.2.1 Single-user access granularity**

The DAC/D2 class requires individual access control; therefore, the granularity of user identification must enable the capability to discern an individual user. That is, access control based upon group identity alone is insufficient. To comply with the requirement, the DAC subsystem must either provide unique user identities through its own I&A mechanism or interface with an I&A mechanism that provides unique user identities. The DAC subsystem must be able to interface to an auditing mechanism that records data about access mediation events. The evaluation shall show that audit data is created and is available to the auditing mechanism.

### **2.1.3.2.2 Authorized user-specified object sharing**

The ability to propagate access right to objects must be limited to authorized users. This additional feature is incorporated to limit access rights propagation. This distribution of privileges encompasses granting, reviewing, and revoking of access. The ability to grant the right to grant propagation of access will itself be limited to authorized users.

### **2.1.3.2.3 Default protection**

The DAC mechanism must deny all users access to object when no explicit action has been taken by the authorized user to allow access.

## **-D3**

### **2.1.3.3.1 Access control lists for each object**

The DAC subsystem shall allow users to specify the list of individuals or groups of individuals who can access each object. The list shall additionally specify the mode(s) of access that is allowed each user or group. This implies that access control lists associated with each object is the only acceptable mechanism to satisfy the D3 requirement for DAC.

## **Applicable Features**

Watchdog provides discretionary access control between subjects and objects. Watchdog provides single-user granularity by requiring each user to have a different user identification. The DAC portion of Watchdog interfaces with the audit mechanism to record access mediation events. Only authorized users (SA) may grant access rights to users of the system. Users may share information with other users by moving data to a mutually owned area.

## **Conclusion**

Watchdog satisfies the Discretionary Access Control D2 feature requirement. Watchdog does not satisfy the D3 feature requirement because it does not explicitly provide access control lists.

## **Object Reuse**

### **Requirement**

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

## **Interpretation**

### **- D2:**

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

## **Applicable Features**

In Watchdog there are a number of distinct controlled objects (see page 7, "Objects)." The objects capable of storing information fall into two classes, the file system objects and the memory objects. File system objects are overwritten to prevent the reuse of information after deallocation. Memory objects, with the exception of TSRs are cleared at the end of a user's session. Since only one subject can be active on the system while a given session is in progress, this prevents the scavenging of memory objects.

Watchdog fails to clear ALL memory objects. Specifically, it fails to clear memory for Terminate and Stay Resident (TSR) programs or the buffers associated with the TSR programs. Some of the objects on the underlying system are not controlled.

## **Conclusion**

Watchdog fails to satisfy the Object Reuse feature requirement.

## **Assurances**

### **System Architecture**

#### **Requirement**

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

## Interpretation

### - D1:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

#### 3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

#### 3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

### - D2:

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to all subsystems at the D2 class or the D3 class. The following interpretations explain how this requirement applies to specific functions performed by subsystems.

#### - Interpretation for DAC Subsystems:

All named objects which are in the defined subset of protected objects shall be isolated such that the DAC subsystem mediates all access to those objects.

**- Interpretation for Auditing Subsystems:**

The system's architecture shall ensure that the auditing mechanism cannot be bypassed by any subjects accessing those objects under the system's control.

**- Interpretation for Object Reuse Subsystems:**

The notion of subsetting objects is not applicable to object reuse subsystems. Object reuse subsystems shall perform their function for all storage objects on the protected system that are accessible to users.

**- Interpretation for I&A Subsystems:**

This requirement applies to I&A subsystems. Authentication data shall be protected from unauthorized access. Access to the authentication data shall also be recorded in the audit trail.

## **Applicable Features**

Watchdog isolates itself from user tampering primarily by restrictions on the facilities provided to users by the system. Since Watchdog does not maintain a separate execution domain, it is possible to modify the subsystem if programs that can provide direct access to memory, such as compilers and interpreters, are allowed on the system.

The controlled objects are defined on page 7. Other objects on the PC are accessible and not protected.

## **Conclusion**

Watchdog satisfies the D2 System Architecture requirements.

## **System Integrity**

### **Requirement**

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

### **Interpretation**

#### **- D1:**

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to all subsystems evaluated at any class, regardless of the functions they perform.

### **Applicable Features**

Watchdog provides diagnostics to test the various devices of the Watchdog Armor card.

### **Conclusion**

Watchdog satisfies the System Integrity D2 requirement.

## **Security Testing**

### **Requirement**

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

## Interpretation

### - D1:

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

### - D2:

This requirement applies to the testing of the SRP of any subsystem evaluated at the D2 class or the D3 class.

## Applicable Features

The evaluation team tested Watchdog in two phases, the first focusing on functional testing, and then a second phase of security testing. Watchdog was installed to provide the maximum security available with the product. The functional testing phase concentrated on providing the team assurance that the product was installed properly and functioned consistently with the instructions provided. The security testing phase focuses on determining if there are any apparent ways to bypass or defeat the security mechanisms.

Functional testing is basically testing as the system might be installed in the field, using DOS and any application programs that are not specifically forbidden by the instructions. All optional security features were turned on and several "accounts" were created with varying levels of privileges. The Watchdog system worked as documented with little or no interpretation of the documentation required.

The second phase of testing, security testing, consisted of looking for obvious flaws that would bypass or defeat the Watchdog's protection mechanisms. Watchdog was able to prevent unauthorized access to objects. If the system is properly configured and administered, and users are not allowed access to the floppy drives or to compilers, then the team found no obvious flaws with the Watchdog system.

## **Conclusion**

Watchdog satisfies the Security Testing D2 requirement.

## **Documentation**

### **Security Features User's Guide**

#### **Requirement**

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

#### **Interpretation**

##### **- D1**

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

#### **Applicable Features**

Watchdog supplies a 68 page user's guide which explains the protection mechanisms used. This guide only discusses the operation of unprivileged functions. It includes a very good description of the I&A mechanism used by Watchdog. Because control of file access permissions is restricted to the system administrator, no discussion of these facilities is included in the user guide. There are no additional requirements from D1 to D2.

## **Conclusion**

Watchdog satisfies the D2 Security Features User's Guide requirement.



## **Trusted Facility Manual**

### **Requirement**

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

### **Interpretation**

#### **- D1:**

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

#### **- D2:**

This requirement applies directly to all auditing subsystems and to other subsystems that maintain their own audit data concerning events that happen under their control. For subsystems that create audit data and pass it to an external auditing collection and maintenance facility, the audit record structure shall be documented; however, the procedures for examination and maintenance of audit files may be left to the external auditing facility.

### **Applicable Features**

Watchdog provides a 277 page system administrator's guide to describe the installation and use of the system. The guide contains a chapter on maximizing system security, which the team feels should be followed to meet the requirements of this evaluation.

### **Conclusion**

Watchdog satisfies the Trusted Facility Manual D2 requirement.

## **Test Documentation**

### **Requirement**

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

### **Interpretation**

#### **- D1:**

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

### **Applicable Features**

Fischer supplied test documentation which described the test plan, test procedures and the expected results of the security mechanisms' functional tests. In this documentation Fischer explained the configuration and options selected for the security testing.

### **Conclusion**

Watchdog satisfies the Test Documentation D2 requirement.

## **Design Documentation**

### **Requirement**

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

## Interpretation

### - D1:

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

## Applicable Features

Fischer supplied minimally adequate design documentation. The descriptions of the operation of any given point of the system were superficial. Specifically, the documentation was most likely insufficient for a new developer to understand the structure of the system well enough to maintain it.

## Conclusion

Watchdog satisfies the D2 Design Documentation requirements.

## Rating Assignment

This section describes the composite rating and how it is determined. A composite rating is assigned to each evaluated feature and is based upon the individual ratings issued in Chapter 3. The individual ratings are the rating for each feature and ratings for assurance and documentation supporting that feature. The chart below shows a 'Y' for each assurance or documentation requirement that is sufficient to support the rating of each feature. An 'N' indicates that the assurance or documentation requirement is not sufficient. For features that have a rating of 'D', the assurances and documentation requirements are irrelevant, and are marked 'N/A'. Using the ratings attained in Section 3, the composite ratings for each of Watchdog's features are derived as shown in the following table.

Evaluated Features	Feature Rating	Assurance			Documentation				Supporting Function	Composite Rating
		Arch.	Integrity	Testing	SFUG	TFM	Testing	Design		
I&A	D2	Y	Y	Y	Y	Y	Y	Y	Audit <sup>1</sup> DAC <sup>2</sup>	D2
Audit	D2	Y	Y	Y	Y	Y	Y	Y	I&A <sup>3</sup> DAC <sup>4</sup>	D2
DAC	D2	Y	Y	Y	Y	Y	Y	Y	I&A <sup>5</sup> Audit <sup>6</sup>	D2
OR	D	N/A	N/A	N/A	N/A	N/A	N/A	N/A		D

The CSSI requires that subsystems have *supporting functions* because some features rely on one another (e.g. an auditing subsystem needs user identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

- The supporting function is provided by another feature of the subsystem.
- The supporting function is provided within the feature even though it may duplicate an aspect of another feature.
- The supporting function is provided through an interface to other products

If the supporting function is integrated within the product, it must be at the same level as that of the feature to obtain the composite rating.

---

<sup>1</sup>Authentication data protected on Watchdog board. Watchdog provides sufficient audit capability to support I&A.

<sup>2</sup>Authentication data is stored in the Watchdog system administrator's protected area.

<sup>3</sup>The audit mechanism gets user IDs from the I&A mechanism.

<sup>4</sup>Audit data is maintained in system area and is inaccessible to unprivileged users.

<sup>5</sup>The DAC mechanism gets user IDs from the I&A mechanism.

<sup>6</sup>The DAC mechanism interfaces with the audit mechanism to record access mediation events.

## Evaluator's Comments

This section allows the evaluators to comment on features or problems that the TCSEC and CSSI do not specifically address. This provides a "hands on" perspective which a user of a system may find useful or needed to administer or use the system.

The team feels that Watchdog does provide a level of security which the PC running DOS alone lacks. Although, to maintain this level, the system administrator should only allow privileged users access to the diskettes drives, DOS commands, and programs such as compilers and debuggers. Because of these restrictions Watchdog may not be suitable for a programming environment.

The menu system and documentation was user friendly. The team feels that the points mentioned in the chapter on maximizing security in the System Administrator's Guide should be followed carefully.

The task of deleting a user required looking through several menus to make certain all access privileges had been revoked for the user. The team felt that this process could be simplified.

## **Evaluated Hardware Components**

This appendix lists the Fischer marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluation.

To operate in correspondence with the DAC, I&A, OR, and Audit ratings, the security subsystem must contain the hardware components listed in this section.

The protected system covered by this evaluation is the IBM PC/XT and the IBM PC AT.

## Evaluated Software Components

This section lists the programs that make up the various divisions of Watchdog's software. Watchdog is designed to run under revisions 2.0 or higher of PC-DOS and MS-DOS.

Version 5.2.2 of the Watchdog PC Data Security software and Version 1.1.0 of the Watchdog Armor software was evaluated. The Watchdog PC Data Security software was delivered on four 5 1/4" floppy diskettes <sup>1</sup> along with a User and a System Administrator Tutorial diskettes. The Watchdog Armor card was delivered with one 5 1/4" floppy diskette. The software on these diskettes consisted of the files listed below:

- INSTALL/SYSTEM ADMINISTRATOR DISK VERSION 5.2.2
  - INSTALL.BAT
  - REPLACE.BAT
  - SAD.BAT
  - SAD.HLP
  - UPGRADE.BAT
  - WDSA.EXE
- PROGRAM DISK VERSION 5.2.2
  - DESDVR.SYS
  - KERERR.EXE
  - README.DOC
  - WD.EXE
  - WD.HLP
  - WDAC.EXE
  - WDDRIVER.SYS
  - WDINIT.SYS
  - WDMENBLD.EXE

---

<sup>1</sup>Note: All of Watchdog's software is also available in 3 1/2" micro diskettes.

- WDO.EXE
- AUDIT TRAIL DISK VERSION 5.2.2
  - AUDTRL.HLP
  - WDMAIL.EXE
  - WDPURGE.EXE
  - WDRLIST.EXE
  - WDRMAIN.001
  - WDRMAIN.003
  - WDRMAIN.004
  - WDRMAIN.EXE
  - WDRTRACK.EXE
- SUPPLEMENTAL DISK VERSION 5.2.2
  - KEYLOCK.EXE
  - SA.HLP
  - WD.PIF
  - WDEMUL.EXE
  - WDET.EXE
  - WDREADME.DOC
  - WDRUN.EXE
  - WDRUN.PIF
  - WDVVIEW.EXE
- WATCHDOG ARMOR DISK VERSION 1.1.0
  - INSTALL.BAT
  - README.DOC
  - WDARMOR.BIN
  - WDARMOR.EXE
  - WDARMOR.HLP



## Glossary of Acronyms

<b>ADP</b>	Automatic Data Processing
<b>BIOS</b>	Basic Input-Output System
<b>CPU</b>	Central Processing Unit
<b>CSSI</b>	Computer Security Subsystem Interpretation
<b>DAC</b>	Discretionary Access Control
<b>DOS</b>	Disk Operating System
<b>EMS</b>	Extended Memory Service
<b>EPL</b>	Evaluated Products List
<b>ID</b>	Identification
<b>I&amp;A</b>	Identification and Authentication
<b>MAC</b>	Mandatory Access Control
<b>MS-DOS</b>	MicroSoft Disk Operating System
<b>NCSC</b>	National Computer Security Center
<b>OR</b>	Object Reuse
<b>PC</b>	Personal Computer
<b>RAM</b>	Random Access Memory
<b>ROM</b>	Read Only Memory
<b>SA</b>	System Administrator
<b>SFUG</b>	Security Features User's Guide
<b>SRP</b>	Security Relevant Portion
<b>TCB</b>	Trusted Computing Base
<b>TCSEC</b>	Trusted Computer Security Evaluation Criteria
<b>TFM</b>	Trusted Facility Manual
<b>TSR</b>	Terminate and Stay Resident

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

## REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION <b>UNCLASSIFIED</b>			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT <b>UNLIMITED DISTRIBUTION</b>		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S) <b>CSC-EPL--SUM-90/007</b>			5. MONITORING ORGANIZATION REPORT NUMBER(S) <b>S236,002</b>		
6a. NAME OF PERFORMING ORGANIZATION <b>National Security Agency</b>		6b. OFFICE SYMBOL (If applicable) <b>C71</b>	7a. NAME OF MONITORING ORGANIZATION <b>National Computer Security Center</b>		
6c. ADDRESS (City, State and ZIP Code) <b>9800 Savage Road Ft. George G. Meade, MD 20755-6000</b>			7b. ADDRESS (City, State and ZIP Code) <b>9800 Savage Road Ft. George G. Meade, MD 20755-6000</b>		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8c. ADDRESS (City, State and ZIP Code)			10. SOURCE OF FUNDING NOS.		
			PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.
11. TITLE (Include Security Classification) <b>Final Evaluation Report Fischer Intl Systems Corp Watchdog</b>					
12. PERSONAL AUTHOR(S) Deborah M. Clawson; Michael J. Oehler; Shawn M. Rovanseck					
13a. TYPE OF REPORT <b>Final</b>		13b. TIME COVERED FROM ____ TO ____		14. DATE OF REPORT (Yr, Mo., Day) <b>901001</b>	
15. PAGE COUNT <b>34</b>					
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) <b>NCSC, I&amp;A, DAC, AUD, OR, Fischer Intl, Watchdog, CSSI</b>		
FIELD	GROUP	SUB GR			
19. ABSTRACT (Continue on reverse side if necessary and identify by block number) <b>The Fischer International Systems Corporation Watchdog has been evaluated by the National Computer Security Center (NCSC). The security features of Watchdog were examined against the requirements specified by the COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988. The NCSC evaluation team has determined that Watchdog satisfies the requirement for I&amp;A/D2, DAC/D2, AUD/D2, and OR/D. It has been determined that the highest class at which the EIS System satisfies all the specified requirements of the CSSI is class I&amp;A/D2, DAC/D2, AUD/D2, and OR/D.</b>					
<b>This report documents the findings of the evaluation.</b>					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <b>UNCLASSIFIED/UNLIMITED</b>			21. ABSTRACT SECURITY CLASSIFICATION <b>UNCLASSIFIED</b>		
22a. NAME OF RESPONSIBLE INDIVIDUAL <b>PATRICIA L. MORENO</b>			22b. TELEPHONE NUMBER (Include Area Code) <b>(301)859-4458</b>		8b. OFFICE SYMBOL <b>C71</b>